not be construed as limited to the embodiments set forth herein. Rather these embodiments are provided so that this disclosure will be thorough and complete and will fully convey the invention to those skilled in the art.

[0040] In an embodiment of the present invention, an identity provider is an entity that creates, maintains, and manages identity information for principals and other system entities. Identity information includes user attributes such as name, mailing address, e-mail address, and telephone number. User attributes can be further assembled into user profile data to provide additional flexibility and personalization. For example, a "personal" profile contains attributes such as social security number, credit card data, billing address, and affinity memberships (e.g., frequent flyer numbers). A "work" profile contains attributes such as work address, work telephone numbers, and work e-mail address. Identity information further includes preferences or policies that describe permissible (or impermissible) uses of user attributes or profile data. Identity information is described in further detail below and with reference to FIG. **24**. In an embodiment, a service provider is an entity that provides a service to a principal and makes use of the aspects of a principal's identity it has been authorized to access. A principal is a system entity whose identity can be authenticated. One example of a principal is a natural person functioning as an end user.

[0041] A. System Architecture

[0042] FIG. **1** is an illustration of a distributed identity system in accordance with the present invention. The illustrated embodiment shows system entities such as identity provider A **105**, identity provider B **110**, service provider A **115**, service provider B **120**, and user **125** each coupled to network **130**. Further, identity provider B **110** and service provider B **120** are separately coupled to one another. This system architecture enables, for example, identity provider A **105** to communicate with service provider B **120** across network **130**. Network **130** is configured to provide connection-oriented or connectionless connectivity to the communicating nodes. For example, identity provider B **110** can communicate with service provider B **120** through network **130** and via the illustrated peer connection. In an embodiment, system entities such as identity provider A **105** and service provider A **115** are in distinct domains and interact using the hypertext transport protocol (HTTP). Exemplary details of interaction between an identity provider and a service provider to enable distributed network identity are described below.

[0043] In an embodiment, a system entity is a process that incorporates a distinct set of functionality. For example, identity provider A **105** incorporates functionality to create and to maintain identity information. The functionality of a system entity can be implemented by program instructions that execute in an appropriate computing device. One skilled in the art will recognize that numerous computing devices are appropriate for the illustrated system architecture. Example devices include enterprise servers (e.g., Sun Fire 15K, commercially available from Sun Microsystems, Inc., Santa Clara, Calif.), application servers, workstations, personal computers, network computers, network appliances, personal digital assistants, game consoles, televisions, set-top boxes, premises automation equipment, point-of-sale terminals, automobiles, and personal communications devices (e.g., cellular handsets). The program instructions can be distributed on a computer readable medium or storage volume. The computer readable storage volume can be available via a public network, a private network, or the Internet. Program instructions can be in any appropriate form, such as source code, object code, or scripting code.

[0044] In an embodiment, network **130** is a partially public or a wholly public network such as the Internet. Network **130** can also be a private network or include one or more distinct or logical private networks (e.g., virtual private networks). Additionally, the illustrated communication links to network **130** and between identity provider B **110** and service provider B **120** can be wireline or wireless (i.e., terrestrial- or satellite-based transceivers).

[0045] Although they are distinctly illustrated, in certain embodiments, multiple system entities can be hosted by a single computing device or group of computing devices functioning as a virtual machine (e.g., a clustered configuration). For example, a server can host both identity provider B **110** and service provider A **115**. That is, a trusted entity, such as a banking institution, can be an identity provider for its customers, as well as provide online services. Similarly, computing devices coupled to network **130** can be configured to host identity provider A **105** and service provider B **120**. One skilled in the art will recognize that depending on configuration, system entities communicate locally using a protocol such as HTTP, by interprocess communication, or by some other means. Although user **125** is singularly illustrated, embodiments of the present invention support a plurality of concurrent users. User **125** can be a principal, such as a natural person, computer program, or user agent. Similarly, embodiments include a plurality of service providers and identity providers operating concurrently on network **130**. One skilled in the art will recognize that methods, apparatus, systems, data structures, and computer program products implement the features, functionalities, or modes of usage described herein. For instance, an apparatus embodiment can perform the corresponding steps or acts of a method embodiment.

[0046] In an embodiment, single sign-on refers to the ability of an entity to be authenticated sufficiently to gain access to all authorized, secured resources throughout one or more systems without additional authentication. A number of factors affect how much access an entity achieves using single sign-on including the type of authentication provided and the service provider's access control policy. In the illustrated embodiment, for example, user **125** can authenticate with identity A provider **105**, obtain an assertion from identity provider A **105**, and present the assertion to service provider A **115**. An authentication assertion conveys information about an act of authentication. Once user **125** has authenticated with identity provider A **105**, user **125** can use service provider A **115** and other service providers (e.g., service provider B **120**) without having to login or to sign on again. Advantages of single sign-on for user **125** include convenient access to service providers and account management flexibility. As further described below, the system architecture enables a user to distribute identity information among identity providers and to control how the identity information is shared and accessed.

[0047] Embodiments of the present invention include single sign-on, federated identity, and web services features.